NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Missile component damaged in accident. A U.S. Air Force (USAF) crew damaged a component of an unarmed intercontinental ballistic missile while performing maintenance near a North Dakota base November 17, prompting a partial evacuation, military officials said December 5. USAF officials said no one was hurt in the incident near Minot Air Force Base, but it was immediately reported to the highest levels of the Pentagon. USAF officials said they initially decided to withhold information about the lapse because it did not pose a risk to public safety, and because they wanted to avoid needless alarm over nuclear weapons safeguards. They confirmed the incident December 5 in response to queries from the Washington Post. A spokesman for the USAF's Global Strike Command said technicians were conducting "routine maintenance" on a section of a Minuteman III missile when a "small replaceable component" was damaged. He said the component, which he would not describe for security reasons, was not attached to the missile. He said the missile was not armed with a warhead at the time, and that no nuclear materials were involved. Source: http://www.washingtonpost.com/world/national-security/missile-component-damaged-in-accident/2011/12/05/gIQArdroXO_story.html

Regional

Minn. gets new setback in fight against Asian carp. Tests have found signs of Asian carp in the Mississippi River north of a key physical barrier keeping the invasive species of fish from spreading into many of Minnesota's most popular lakes, officials said December 8. The sensitive tests detected DNA from silver carp in the water above the Coon Rapids Dam, which is upstream from Minneapolis, the Minnesota Department of Natural Resources said. Nineteen out of 48 water samples taken near the dam in September tested positive for silver carp DNA, and three of the positive results were from above the dam. No live Asian carp have been caught there yet, and experts are not ruling out the possibility of false positives. Source: http://www.salon.com/2011/12/08/minn_gets_new_setback_in_fight_against_asian_carp/

(Minnesota) **Maple Grove teacher on leave after science class explosion.** A Maple Grove Junior High science teacher is on paid leave while the school district investigates an experiment mishap that burned four students in Maple Grove, Minnesota, KMSP 9 Eden Prairie reported December 5. Three students were treated and released from Hennepin County Medical Center for burns they received in the methanol-fueled explosion December 1. A fourth student suffered severe burns to his face and was hospitalized until the weekend of December 3 and December 4. Source: http://www.myfoxtwincities.com/dpp/news/matt-achor-maple-grove-teachr-leave-methanol-dec-5-2011

(South Dakota) **Outage hits AT&T wireless customers in central South Dakota; cut fiber optic line is blamed.** A cut Century Link fiber optic line was blamed for an outage that affected AT&T wireless customers in South Dakota December 6. KCCR 1240 Pierre reported voice and data services were disrupted for about 7 hours December 6. Police in Pierre said there was no apparent disruption to the emergency 911 system in the capital city. The state public utilities

commission gathered information December 7 about the outage that ended about 11 p.m. December 6. Source: http://www.aberdeennews.com/news/sns-bc-sd--cellserviceoutage,0,4108517.story

(Wyoming) **EPA study says hydraulic fracturing likely contaminated drinking water in Wyoming town.** The Environmental Protection Agency (EPA) announced December 8 it suspects hydraulic fracturing in a shallow natural gas well in Wyoming contaminated a town's drinking water. After 3 years of study, the agency concluded chemicals found in the aquifer and in individual wells were consistent with those used in hydraulic fracturing. The agency issued a report that will be open for public comment and scientific review. If it is finalized with the same conclusions, it could provide the first documented case where "fracking" contaminated groundwater. Though there have been incidents in which "flowback" water used in a well was improperly handled, the industry has countered criticisms by saying there had not been a documented case where the process itself caused contamination. The EPA study in Pavillion, Wyoming, began in 2008 after residents complained their water smelled and tasted bad. The residents lived near a gas field controlled by Encana, a Canadian energy company. According to the EPA, the agency constructed two monitoring wells to sample water in the aquifer. "EPA's analysis of samples taken from the agency's deep monitoring wells in the aquifer indicates detection of synthetic chemicals, like glycols and alcohols consistent with gas production and hydraulic fracturing fluids, benzene concentrations well above Safe Drinking Water Act standards, and high methane levels," the agency said in a statement. Source: http://newsok.com/epa-study-says-hydraulic-fracturing-likely-contaminated-drinking-water-in-wyoming-town/article/3630442

National

Nothing Significant to Report

International

Anarchists claim letter bomb at Italy tax office; same group hit Deutsche Bank. A letter bomb exploded December 9 at an office of Italy's tax collection agency, wounding the organization's director. Police said an Italian anarchist group that sent a letter bomb to Deutsche Bank in Frankfurt, Germany, December 7 claimed responsibility. A Rome police official said the December 9 bomb was contained in a yellow bubble envelope mailed to the director's attention at an Equitalia office outside Rome. The tax agency director underwent surgery after suffering injuries to a hand and his face, caused when a glass desktop was shattered by the explosion, an Equitalia official told the ANSA news agency. Italy's Anarchist Federation claimed responsibility. The note included in the package was "very similar" to that contained in the Deutsche Bank letter bomb, which did not explode, a police official said. The group, known in Italy as FAI, warned in its Deutsche Bank note there would be three "explosions" in its latest campaign. Last year around Christmas, the anarchist group sent package bombs to three Roman embassies, injuring two. On December 7 in Frankfurt, a routine mailroom screening found a bomb in a small package addressed to the Deutsche Bank chief executive officer. The

explosive was deactivated without incident. Tucked next to the bomb was a letter of responsibility. Written in Italian, it promised "three explosions against banks, bankers, ticks and bloodsuckers," according to the Hesse state criminal office. Germany's federal prosecutors' office, responsible for national security and terrorism probes, said December 9 it is taking over the investigation. The letter contained about 50 grams of explosive and a fully functional trigger, it said. Source: http://www.washingtonpost.com/world/europe/italian-police-say-package-bomb-explodes-at-tax-collection-office-in-rome-injuring-1/2011/12/09/gIQAWzfihO_story.html

Letter bomb sent to Deutsche Bank chief. German authorities said December 8 a letter bomb addressed to the chief executive of Deutsche Bank in Frankfurt, Germany, contained a fully functional bomb, capable of exploding had it not been intercepted in the bank's mailroom. The bomb was intercepted after a routine X-ray screening December 7 in the mailroom of the bank's Frankfurt headquarters, prosecutors and police from Hesse state said in a joint statement. The authorities refused to give details on the matter, citing an ongoing investigation. A Deutsche Bank spokesman said the bank alerted police immediately after the package came to the attention of mailroom workers during a routine screening. The New York City Police Department (NYPD) said it was alerted to the scare late December 7, causing the department to dispatch patrols to the bank's offices in the city "solely as a precaution." A NYPD spokesman said the return address on the letter was the European Central Bank — the governing body for the 17-nation common European currency, which has its headquarters just across the park from Deutsche Bank in downtown Frankfurt. Source: http://www.cbsnews.com/8301-202_162-57339174/letter-bomb-sent-to-deutsche-bank-chief/

Banking and Finance Industry

CFTC tightens limits on brokerages using customer funds. The Commodity Futures Trading Commission (CFTC) unanimously approved tighter limits on how brokerage firms can use customer funds December 5, a measure the now-bankrupt MF Global encouraged the agency to delay. The CFTC rule prevents brokerage firms, known as futures commission merchants, from conducting "in-house" repurchase transactions and restricts them from investing customer money in foreign sovereign debt. It is not clear whether the rule would have prevented MF Global from misappropriating as much as $1.2 billion in customer money, in what regulators believe was an unprecedented breach of client funds. It appears the push to finalize the rule gained momentum after the brokerage's collapse shook faith in regulators' ability to protect commodity traders. The measure was finalized in a 5-0 vote. It was initially in October 2010, but stalled because there was not enough commissioner support. The agency also passed two lesser-known measures as it races to put in place the sweeping overhaul of U.S. financial regulations ordered by 2010's Dodd-Frank law. It is well behind schedule having implemented some 20 rules so far, with most of the high-profile and controversial rules yet to come. Currently, futures commission merchants are allowed to engage in internal repurchases, or "repo" agreements. The transactions allow firms to take customer funds and invest them in a range of securities such as sovereign debt. Under the new rule, the agency will permit companies to invest consumer funds in securities such as Treasuries, agency debt, corporate

notes, and commercial paper. Potentially risky foreign sovereign debt will no longer be permitted. Transactions between affiliates of a company where the two entities exchange money or funds also are restricted by the new rule. Firms would still be able to enter into agreements using customer funds with an external third party. Source: http://www.reuters.com/article/2011/12/05/us-financial-cftc-meeting-idUSTRE7B410420111205

SEC touts its crackdown on insider trading. Even as it fends off criticism in other areas, the Securities and Exchange Commission (SEC) is pointing to its crackdown on insider trading as proof of its effectiveness. Always a high priority, the agency significantly boosted the number of cases brought against Wall Street traders and hedge-fund managers, according to data it released to Congress late the week of November 28. The SEC said it lodged 53 cases against 138 people and corporate entities in fiscal 2010, a 43 percent increase from 2009. It said it filed 57 cases against 124 people and entities in fiscal 2011. The agency also developed new investigative techniques, including the creation of a market abuse unit that focuses on a variety of practices, including complex insider-trading cases, the agency enforcement chief told the Senate Committee on Homeland Security and Governmental Affairs. Source: http://latimesblogs.latimes.com/money_co/2011/12/sec-crackdown-insider-trading.html

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

International Checkout hacked, customer credit cards abused. International Checkout customers received e-mails that alert them to the fact the organization has recently fallen victim to a cyberattack which resulted in the theft of a large quantity of personal information, including credit card details, Softpedia reported December 6. It seems the breach was discovered sometime in mid-September, and an investigation was immediately started. Besides the fact that the authorities were notified of the issue, the credit card information from the databases was removed to make sure no one still had access. Even though the information was encrypted, the attacker managed to obtain the encryption key that was stored in a separate location. The company is advising customers to closely monitor their bank account statements for any suspicious transactions. Bank account numbers were not exposed, but credit cards numbers were, and in some situations the financial institutions involved may recommend changing the account number. Source: http://news.softpedia.com/news/International-Checkout-Hacker-Customer-Credit-Cards-Abused-238650.shtml

Communications Sector

Nothing Significant to Report

Critical Manufacturing

NHTSA recall notice - Ford Fusion and Mercury Milan wheel studs. Ford announced a recall December 5 of 128,616 Ford Fusion and Mercury Milan vehicles equipped with 17-inch steel wheels and built from April 1, 2009 through April 30, 2009, and from December 1, 2009 through November 13, 2010. The wheel studs may fracture, potentially causing a wheel to separate. While driving, multiple stud fractures could occur at the wheel location, and the operator may experience vibration and/or wheel separation, increasing the risk of a crash. Ford will notify owners, and dealers will inspect the rear brake disc surface for flatness and replace the discs as necessary. Additionally, the wheel lug nuts will be replaced on all four wheels. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V574000&summary=true&prod_id=664803&PrintVersion=YES

Defense/ Industry Base Sector

Iran shows off downed U.S. spy drone on TV as U.S. assesses loss of technology. The downed Lockheed Martin RQ-170 Sentinel spy drone, which is designed to be virtually invisible to radar and carries advanced communications and surveillance gear, made a 2 and a half minute television debut December 7 on Iran's state-owned Press TV channel. U.S. intelligence officials are assessing the apparent loss of its highly classified technology. The official Iranian Republic News Agency reported the foreign ministry December 7 protested the "violation of Iran's airspace by a U.S. spy drone on [December] 4," the day Iranian forces claimed to have shot down the aircraft, 140 miles inside the Iranian border from Afghanistan. Several U.S. officials said the greatest concern is access to the aircraft could give Russian or Chinese scientists insight into its flight controls, communications gear, video equipment, and any self-destruct or return-to-base mechanisms. In addition, they said, the remains of the RQ-170 could help a technologically sophisticated military or science establishment develop infrared surveillance and targeting technology that under some conditions are capable of detecting stealth aircraft such as drones, and the new Lockheed Martin F-35s. Source: http://www.bloomberg.com/news/2011-12-09/iran-shows-off-downed-spy-drone-as-u-s-assesses-technology-loss.html

Symantec confirms Flash exploits targeted defense companies. Security researchers at Symantec confirmed December 7 that exploits of an unpatched Adobe Reader vulnerability targeted defense contractors, among other businesses. "We've seen [this targeting] people at telecommunications, manufacturing, computer hardware and chemical companies, as well as those in the defense sector," said a senior security manager in Symantec's security response group. Symantec mined its global network of honeypots and security detectors — and located e-mail messages with attached malicious PDF documents — to reach that conclusion. Adobe warned Reader and Acrobat users hackers were exploiting a "zero-day" bug on Windows PCs December 6, crediting Lockheed Martin's security response team and the Defense Security Information Exchange (DSIE), a group of major defense contractors that share information about computer attacks, with reporting the vulnerability. Symantec found attack e-mails dated

November 1 and November 5. It also published an image of a redacted e-mail of the attack's bait — the promise of a 2012 guide to policies on new contract awards — that it said was a sample of the pitches that tried to dupe recipients into opening the attached PDF. Opening the PDF also executed the malicious code — likely malformed 3-D graphics data — compromising the targeted PC and letting the attacker infect the machine with malware. That malware, Symantec's senior security manager said, was identical to what was used in early 2010 by hackers exploiting a then-unpatched bug in Microsoft's Internet Explorer 6 (IE6) and IE7. Symantec labeled the malware "Sykipot" in 2010. "[The malware] is a general-purpose backdoor. One of the interesting things about it is it uses a form of encryption of the stolen information, which helps the attack hide what information is stolen," the security manager said. Sykipot encrypts the pilfered data after it has been retrieved, but while it is still stored on the company's network, as well as when it is transmitted to a hacker-controlled server. Those command-and-control servers are still operating, the manager said. Because of the similarities — using Sykipot, which is not widely in play, and exploiting zero-day vulnerabilities — Symantec suspects the same group of hackers who launched the attacks against IE6 and IE7 in 2010 were also responsible for the Reader-based attacks seen in November. Source: http://www.computerworld.com/s/article/9222496/Symantec_confirms_Flash_exploits_targeted_defense_companies?taxonomyId=17

F-22 production line back on track: Lockheed. Lockheed Martin said their F-22 Raptor production line is back on track after the U.S. Air Force's fleet-wide grounding of the jet disrupted deliveries to the service, Defense News reported December 6. We are delivering jets," said a Lockheed spokeswoman. "The last one delivered was 4185. 4195 will be delivered in late spring 2012." Tail number AF 09-4185 has technically been delivered with the signing of a DD-250 form, but the fifth-generation fighter is currently undergoing government flight tests. After the completion of the tests the week of December 5, the Air Force's 1st Fighter Wing will fly the jet to Langley Air Force Base in Virginia, where it will be based. Source: http://www.defensenews.com/story.php?i=8490569&c=AME&s=AIR

Emergency Services

US, Canada announce comprehensive border security plan. The U.S. President and Canadian prime minister announced an ambitious and far-reaching joint Beyond the Border (BTB) Action Plan December 7 designed to strengthen mutual border security, improve the sharing of threat intelligence, and enhance disaster resilience –- the ability to mitigate, respond to, and recover from catastrophic disruptions. The planwas first announced February 4, when the U.S. President and prime minister initially put forth their respective governments' plans, saying "we share responsibility for the safety, security, and resilience of the United States and of Canada in an increasingly integrated and globalized world." According to a "fact sheet" about the new joint US/Canadian border plan released by the White House, "the BTB Action Plan sets out joint priorities for achieving a new long-term security partnership in four key areas, guided by mutual respect for sovereignty and our separate constitutional and legal frameworks that protect individual privacy." The plan includes addressing threats early; promoting trade facilitation, economic growth, and jobs; strengthening cross-border law enforcement; and protecting

shared critical infrastructure, including enhancing continental and global cybersecurity. Source: http://www.hstoday.us/industry-news/general/single-article/us-canada-announce-comprehensive-border-security-plan/8bcf73612fd99536956b506feab517fe.html

(Virginia) **Official: Virginia Tech gunman who killed cop believed to be dead.** The gunman who killed a police officer December 8 after being pulled over in a traffic stop at Virginia Polytechnic Institute and State University (Virginia Tech) in Blacksburg, Virginia, is believed to be dead, a law enforcement official told the Associated Press. Virginia Tech officials said on the school's Web site that a weapon was recovered near a second body found in a parking lot on campus. It was not immediately clear if the second body was that of the gunman. School officials also said there was no longer an active threat that afternoon and that normal activities could resume. The officer's shooting prompted a lockdown that lasted for hours. As police hunted for the killer, the school applied the lessons learned nearly 5 years ago, warning students and faculty members via e-mail and text message to stay indoors. It was the first gunfire on campus since 33 people were killed in the deadliest mass shooting in modern U.S. history. The university sent updates about every 30 minutes, regardless of whether they had any new information, a school spokesman said. The campus was quieter than usual because classes ended December 7 and students were preparing for exams, which were to begin December 9. The school postponed those tests. The shooting came soon after the conclusion of a hearing where Virginia Tech was appealing a $55,000 fine by the U.S. Education Department in connection with the university's response to the 2007 rampage. Since the massacre, the school expanded its emergency notification systems. Alerts now go out by electronic message boards in classrooms, by text messages, and other methods. Other colleges and universities have put in place similar systems. Universities are required under the Clery Act to provide warnings in a timely manner and to report the number of crimes on campus. During about a 1-hour period during the December 8 incident, the university issued four separate alerts. Source: http://www.suntimes.com/9324302-417/official-virginia-tech-gunman-who-killed-cop-believed-dead.html

(New Hampshire) **Escaped prison inmate reportedly captured in New Hampshire.** A burglary suspect who escaped from a New Hampshire jail 5 days earlier and vowed revenge on two people in Maine was caught December 6, police said. The escapee was captured the evening of December 6 by U.S. marshals near a grocery store in Rochester, New Hampshire, where he had been picked up in a vehicle by a friend, a Maine state police spokesman said. The escapee did not have a gun, like authorities had suspected, and was arrested without incident. The inmate escaped from an Ossipee, New Hampshire, jail December 1 by scaling a razor-wire fence in the recreation yard. Police believed he had a gun and appeared to hold a grudge against two people with whom he once had a personal relationship. The inmate's father was arrested December 2 and was charged with hindering apprehension after being accused of leaving supplies for his son outside his Alfred, Maine home. Police said the package included food, water, medical supplies, blankets, and clothing. The inmate stole a car in Wakefield, New Hampshire, after escaping from jail, police said. The vehicle was found abandoned on a logging road in Alfred. Source: http://www.foxnews.com/us/2011/12/06/escaped-prison-inmate-reportedly-captured-in-new-hampshire/

(New York) **Man walks into B'klyn stationhouse with fake 'bomb'.** A man walked into a stationhouse in the Bay Ridge section of Brooklyn, New York City, December 4 and claimed he was carrying an explosive device. "I have a bomb!" the 40-year-old allegedly shouted when he entered the 68th Precinct's headquarters, police sources said. Police whisked him outside and told him to leave the "bomb," which was wrapped in a bag, on the street. The officers notified the emergency service unit in an adjoining building, and the New York City Police Department Bomb Squad also responded to secure the scene and shut down the block. Inside the bag was an empty propane tank, part of a lamp, and a section of circular hose, sources said. As he was taken into custody, the man said he had planted another bomb in a blue van parked outside a building located about 2 miles away on Fort Hamilton Parkway near 83rd Street. Police rushed to the scene and evacuated the building. They then checked the van but found nothing suspicious, and residents were allowed to return to their apartments. The man is charged with placing a false bomb and making terrorist threats, both felonies. He was taken to Lutheran Hospital for a psychiatric evaluation. Source: http://www.nypost.com/p/news/local/brooklyn/man_tells_klyn_firehouse_he_has_fPQMnHqLhVte3P5v02uDYJ?CMP=OTC-rss&FEEDNAME=

(Michigan) **Hutaree member pleads guilty; FBI report released.** On December 5, the FBI released a report which offers a first-of-its-kind glimpse into the inner workings of the Hutaree militia group accused of plotting a violent anti-government revolt in the backwoods of southeastern Michigan. The report was disclosed on the same day one of the group's members pleaded guilty to his role in the plot, admitting he was a Hutaree member, and one of the group's goals was to use explosive bombs against local and federal law enforcement officers. His admissions mirrored the conclusions of the FBI report. The report cited the findings of a confidential informant who had infiltrated the group, and suspected an attack was imminent. On December 5, nearly 2 years later, one of the members cut a deal with the government in admitting to his role in the plot — a confession that will land him in prison for 5 years. The deal spared him a potential life sentence. The remaining eight defendants are scheduled to go on trial February 7. Source: http://www.freep.com/article/20111206/NEWS01/112060341/Hutaree-member-pleads-guilty-FBI-report-released

ENERGY

Methane pipe problem means soaring electric bill for MMSD. The Milwaukee Metropolitan Sewerage District has received an unexpected utility bill of $4,000 a day since early November as it buys electricity for the South Shore sewage treatment plant in Oak Creek, Wisconsin to replace energy customarily generated with methane, district officials said December 5. The expense amounted to an estimated $84,000 last month, but the unbudgeted bill could soar to a total of $448,000 by the end of February if repairs to the plant's methane gas distribution system require a projected 3 additional months to complete. In November, South Shore plant workers were repairing a section of corroded iron pipe used to drain water vapor from other pipes in the system when they determined corrosion problems were more widespread,

according to the district technical services director. Methane was leaking from an undetermined location, so the network of pipes used to deliver gas to above ground storage tanks and turbine generators was shut down for safety reasons. Methane continues to be produced at the sewage plant, and the volume that cannot be burned in turbines — 13 million cubic feet of the gas in November — is burned in two flares because there is no place to store it. The district's commission held a special meeting December 5 to approve spending up to $235,000 to replace all of the 375 feet of 3-inch drain pipe. A private operator of district facilities, was hired to do the work and study the condition of 600 more feet of larger gas distribution pipe at the plant. Source: http://www.jsonline.com/news/milwaukee/methane-leak-means-soaring-electric-bill-for-sewer-district-9c3anle-135058523.html

MIT study shows U.S. must protect power grid from cyberattacks. The United States needs standards to guard against cyber attacks on power lines that run to homes and businesses, according to a Massachusetts Institute of Technology (MIT) report released December 5. Federal standards to secure the nation's high-voltage electricity grid against sabotage from hackers, disgruntled employees, and terrorists do not cover almost 6 million miles of lower-voltage power lines, according to the study. The study focuses on challenges to the U.S. power network over the next two decades, including the addition of renewable sources of energy, such as wind and solar power, and electricity pricing. U.S. officials are studying whether reliability may be jeopardized by attacks on the network or by Environmental Protection Agency rules, which utilities say will force them to shut down some generating plants fueled by coal and oil. The MIT study also calls for designation of a single federal agency to combat cyber attacks on the U.S. power network. Source: http://fuelfix.com/blog/2011/12/05/mit-study-shows-u-s-must-protect-power-grid-from-cyberattacks/

Food and Agriculture

Listeria Cantaloupe outbreak ends as most deadly in 100 years. A 28-state Listeria outbreak is over, with the distinction of being the most deadly outbreak of food-borne illness in the United States in 100 years, Food Safety News reported December 9. In the end, one out of every five of the victims died from the Listeria contamination spread by a locally grown but widely distributed variety of cantaloupes from Colorado. Thirty of 146 persons infected died. A miscarriage suffered by an Iowa woman was also blamed on outbreak-related listeriosis. The Colorado Department of Public Health and Environment received the first report of a Listeria infection in September. The news of the first fatalities coincided with Jensen Farms recalling all the Rocky Ford-brand cantaloupes it had shipped for the season — at least 1.5 million melons. CDC's final report said only two other produce outlets, Kansas-based Carol's Cuts and New York-based Fruit Fresh Up, recalled product. Those companies had purchased whole cantaloupes from Jensen Farms and cut them up for retail sale. The onset of illnesses was from July 31 to October 27. The U.S. Food and Drug Administration previously reported that its investigation found Listeria contamination on cantaloupes and equipment at the Jensen Farms packing facility in Granada, Colorado. Source: http://www.foodsafetynews.com/2011/12/listeria-outbreak-ends-as-most-deadly-in-100-years/

Cargill recalls dog food for elevated aflatoxin levels. In another recall of dry dog food for elevated levels of aflatoxin, Cargill Animal Nutrition December 7 said it was pulling two regional brands of its dry dog food — River Run and Marksman. Aflatoxins are produced by Aspergillus, a common fungus that can be the result of moldy corn or other grains. The recalled dry dog food, which was manufactured at Cargill's Lecompte, Louisiana, facility between December 1, 2010, and December 1, 2011, and distributed in Kansas, Missouri, Northeast Oklahoma, Arkansas, Louisiana, Mississippi, Tennessee, Western Kentucky, Southeast Indiana, Southern Illinois, Hawaii, Guam, the U.S. Virgin Islands, and limited areas of Florida and California. Source: http://www.foodsafetynews.com/2011/12/cargill-recalls-dog-food-for-elevated-aflatoxin-levels/

Uncle Ben's rice recalled. Mars Food U.S. issued a recall December 7 for its Uncle Ben's Whole Grain White Rice Garden Vegetable product because it contains undeclared milk. The company said the recall affects two date codes of the boxed rice sold in 31 states. The undeclared milk can pose a serious health risk to people who have an allergy or severe sensitivity to milk. Source: http://www.kdvr.com/news/kdvr-uncle-bens-rice-recalled-20111207,0,6555935.story?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+kdvr-news+(KDVR+-+Local+News)

Some Iams dry dog food recalled. A production lot of dry Iams dog food was recalled due to high aflatoxin levels, according to Iams manufacturer, the Procter & Gamble Co. Procter & Gamble said no illnesses had been reported, but advised consumers who purchased the recalled product to stop feeding it to their pets and to discard it. Aflatoxin is a naturally occurring mycotoxin from the growth of various species of Aspergillus, a fungus, and can be harmful to pets' livers, or fatal if consumed in significant quantities. Source: http://www.foodsafetynews.com/2011/12/production-lot-of-iams-dry-dog-food-recalled/

Radioactive cesium in Meiji milk spurs recall. Radioactive cesium was found in milk powder made by a Meiji Holdings Co. unit in Japan raising concern that radiation from a nuclear plant is contaminating baby food, Bloomberg reported December 6. Meiji found traces of cesium-137 and cesium-134 in batches of “Meiji Step” made in March, the Tokyo-based company said. Levels in the 850-gram cans are within safety limits and do not pose a health risk. The investigation was made following a complaint from a consumer in November. The finding highlights the radiation threat to food in Japan 9 months after the Fukushima nuclear plant was wrecked by an earthquake and tsunami. Prolonged exposure to radiation in the air, ground, and food can damage DNA, causing leukemia and other cancers. While infants are especially susceptible, the milk powder may not be a significant threat if contamination is limited to small quantities in isolated batches, said a food safety consultant. The company is recalling 400,000 cans of “Meiji Step,” a powdered milk formulated for babies older than 9 months, packaged in April and mostly distributed in May. Source: http://www.bloomberg.com/news/2011-12-06/radioactive-cesium-found-in-meiji-baby-formula-spurs-recall-shares-fall.html

Government Sector (including Schools and Universities)

Error could cause thousands of TWIC cards to be rejected. The Transportation Security Administration (TSA) indicated some 26,000 holders of the Transportation Worker Identification Credential (TWIC) may not be able to use their cards at an electronic reader because of an encoding error, the Journal of Commerce reported December 6. The TWIC is a tamper-resistant biometric credential for maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002, and all U.S. Coast Guard-credentialed merchant mariners. The TSA said a system error caused a federal code number to be incorrectly embedded on the card's microchip, and the agency said the error was fixed April 5. The TSA did not say why it took until November to notify holders. TWIC holders who received cards before April 5 "could potentially" have it rejected by an electronic reader, the TSA said. Right now, only a handful of ports and terminals have electronic readers working. All told, the TSA has issued 1.8 million TWICs. The agency has published a list of card serial numbers that may have the encoding problem. The agency will replace cards free of charge. However, if the credential is being used at locations without a reader, the holder does not have to replace it right way. Source: http://www.joc.com/portsterminals/error-could-cause-thousands-twic-cards-be-rejected

Information Technology and Telecommunications

Feds launch cloud security standards program. Federal agencies will soon have a government-wide security standard for assessing, authorizing and monitoring cloud products and services. The Federal Chief Information Officer December 8 unveiled the Federal Risk and Authorization Management Program (FedRAMP), which establishes a set of baseline security and privacy standards all cloud service providers will need to meet to sell their products to government agencies. The program requires that all agencies use only FedRAMP-certified cloud services and technologies for public clouds, private clouds, hybrid clouds, and community clouds. The program also covers all cloud service models, including Software as a Service (SaaS) and Platform as a Service (PaaS). FedRAMP will also provide federal agencies with standard procurement language to use in requests for proposals from cloud service vendors. A Joint Authorization Board, comprising of security experts from the DHS, General Services Administration, and the Department of Defense will be responsible for updating the FedRAMP security requirements on an ongoing basis. A group of third-party assessors hired from the private sector will be responsible for independently assessing cloud service providers and certifying their compliance with the standards. Source: http://www.computerworld.com/s/article/9222525/Feds_launch_cloud_security_standards_program?taxonomyId=17

XSS vulnerabilities can affect embedded browsers in mobile apps. A security researcher has noted the use of embedded browsers in mobile applications can make those applications vulnerable to cross site scripting (XSS) attacks, H Security reported December 7. Developers of

mobile software found it can be effective to embed a smartphone operating system's Web browser and then create their user interface using HTML, CSS, and JavaScript. The user interface is then more portable to other devices and is easier to customize using CSS. However, this convenience comes at a cost. A researcher, who is presenting his findings at TakedownCon, found some developers do not clean the data being sent to their HTML-based user interface. Source: http://www.h-online.com/security/news/item/XSS-vulnerabilities-can-affect-embedded-browsers-in-mobile-apps-1391326.html

Fake Verizon notification carries malware. A spam e-mail campaign aiming to infect users with a banking trojan is currently underway and is targeting mobile carrier customers, Microsoft has warned, Help Net Security reported December 7. The e-mail purports to be coming from Verizon, and tries to make the recipient feel a sense of urgency by claiming it contains important account information from Verizon Wireless. The message starts with the unusual greeting of "Hello Dear!," and proceeds to try and convince the users they have to pay a rather large bill (the amount varies from $250 to over $1,500). "View all your recent bills in application materials," says the e-mail, and offers an attached ZIP file named Verizon-Wireless-Account-StatusNotification_#######.zip, with random numbers used in the name. The archive contains a similarly named executable, which is detected as a variant of the Zeus banking trojan, and Microsoft warns a similar campaign carrying the same payload has already been started using e-mails pretending to deliver a critical update for Adobe Acrobat Reader and Adobe X Suite. Source: http://www.net-security.org/malware_news.php?id=1926

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

FDA panel wants more risk information on Yaz pills. Federal health experts said December 8 that drug labeling for Yaz and other widely-used birth control pills should be updated to emphasize recent data suggesting a higher risk of blood clots with the drugs than older contraceptive pills. The Food and Drug Administration's panel of experts voted 21-5 that labeling on the popular drugs made by Bayer is inadequate and needs more information about the potential risk of blood clots in the legs and lungs. In an earlier vote, panelists voted 15-11 that the pills remain a beneficial option for preventing pregnancy. The majority ruling amounts to a vote of confidence for keeping the drugs on the market, though well over a third of panelists voted against the drug's overall benefit, citing numerous alternatives available. Source: http://www.boston.com/business/articles/2011/12/08/fda_panel_wants_more_risk_information_on_yaz_pills/

Bayer withheld Yasmin data from U.S., former agency chief says. A Bayer AG unit withheld from U.S. regulators findings by company researchers of increased reports of blood clots in users of its Yasmin birth-control pills, the former head of the Food and Drug Administration said. The former FDA commissioner, in a document unsealed December 5 in federal court in Illinois, said Bayer did not include an analysis "that demonstrated an increase in the U.S. reporting rate" for venous thromboembolism (VTE), or clots, in a 2004 review of Yasmin's safety provided to the agency. The report also did not include an earlier draft opinion by company researchers that "spontaneous reporting data do signal a difference in the VTE rates for Yasmin" compared with other oral contraceptives, he said, quoting the draft. The company also promoted the oral contraceptive for unapproved uses, particularly for treatment of premenstrual syndrome. Bayer faces more than 10,000 lawsuits over injuries allegedly caused by the contraceptives. Lawyers suing the drugmaker cited FDA reports of at least 50 deaths tied to the pills from 2004 to 2008. The first trials are scheduled for next month in federal court in Illinois, and state court in Philadelphia, Pennsylvania. Source: http://news.businessweek.com/article.asp?documentKey=1376-LVQYL56S972I01-7V9D1IMKMU35U8DIJ4NU7MFOEJ

Transportation

Nothing Significant to Report

Water and Dams

(Missouri; Illinois) **Corps of engineers warns of flood risk at Birds Point Levee.** The U.S. Army Corps of Engineers said it is likely there will be more flooding along a Mississippi River floodway in southeast Missouri in the near future. Based on forecasts of unseasonably high river levels there is a "significant risk" of more flooding along the Birds Point Floodway that was inundated earlier this year. In May, the Corps blew three holes in the levee to relieve pressure at the height of the Mississippi River flooding that was threatening nearby Cairo, Illinois. About 130,000 acres of farmland were damaged, along with dozens of homes. The Corps said weather patterns that include heavy rains in the region are expected through the middle of December. Higher than usual levels of precipitation are also forecast through spring. Source: http://www.kait8.com/story/16043513/corps-of-engineers-warns-of-flood-risk-at-birds-point-levee

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455;

US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168